REMARKS

Applicants appreciate the Examiner's attention to this application.

This response amends claims 1, 3, 10, 13-15, 22, 25, 27, 34, 37, 39, and 46; and cancels claims 9, 21, 33, and 45. Claims 1, 13, 25, and 37 are the pending independent claims. Reconsideration of the present application in view of the enclosed amendments and remarks is respectfully requested.

ARGUMENT

The Office Action objects to claims 14 and 25 due to informalities. This response corrects those informalities.

The Office Action also includes claim rejections based on 35 U.S.C. §§ 102(e) and 103(a). To the extent that those rejections might be applied to the claims, as amended by this response, Applicants respectfully traverse.

35 U.S.C. § 102(e)

The Office Action rejects claims 1-6, 9-18, 21-30, 33-42, and 45-48 as being anticipated by U.S. patent no 6,327,652 to Paul England et al. (Hereinafter "England").

For a valid rejection under 35 U.S.C. § 102, "[t]he identical invention must be shown in as complete detail as is contained in the ... claim." (MPEP § 2131.01, quoting from Richardson v. Suzuki Motor Co., 9 USPQ2d 1913, 1920 (Fed. Cir. 1989)).

England pertains to a method for identifying the operating system running on a computer, based on "an identity associated with an initial component for the operating system, combined with identities of additional components that are loaded afterwards." In particular, after digital signatures for each component are validated, the operating system (referred to as a "digital rights management operating system" or "DRMOS") may assume a "trusted identity." (Abstract.) As far as it goes, England appears to describe reasonable facets of a possible approach to supporting digital rights management.

The present application involves technology that could also be applied in the arena of digital rights management. However, the present application, and in particular the pending claims, involve many details that England does not disclose.

For instance, claim 13 pertains to a method of using an operating system nub key (OSNK) to protect usage of a subset of a software environment. Further, claim 1 recites that the operation of "protecting usage" involves "encrypting a value while operating in isolated execution mode" and/or "decrypting an encrypted value while operating in isolated execution mode." Thus, claim 13 recites a method in which "isolated execution mode" is used to protect usage of a subset of a software environment.

As explained in the detailed description of the present application, isolated execution mode is a mode of operation in which the platform allows access to a region of system memory that is protected by the platform hardware. Such regions of memory may be referred to as "isolated memory areas" or simply "isolated memory." The platform hardware prevents access to isolated memory when the system is not in isolated execution mode (e.g., when the system is in "normal execution mode"). Furthermore, isolated execution mode is not to be confused with conventional privilege rings. For example, as explained in greater detail in the detailed description, a platform that supports a "normal execution mode" and an "isolated execution mode" may also support privilege rings within the normal execution mode, as well as privilege rings within the isolated execution mode. (FIGs. 1A-1C and page 3, line 8, through page 10, line 27.)

England does not disclose either encrypting a value or decrypting a value "while operating in isolated execution mode." In fact, England does not disclose performing any kind of operations in isolated execution mode. England does not mention isolated execution mode at all. England therefore does not anticipate claim 13.

With regard to original claims 9, 22, 33, and 45, the Office Action asserts that England discloses, at col. 2, lines 47-67, a "secure platform [that] uses an isolated execution mode." Applicants respectfully traverse that assertion.

At col. 2, lines 47-67, England does not disclose a secure platform that uses an isolated execution mode. That portion of England merely indicates that (a) a "secure boot" is a necessary stepping stone to a secure operating system, (b) secure boot of an operating system may be a multi-stage process, (c) at startup, a "trusted program" may load an initial layer of the operating system and may check the integrity of that initial layer, and (d) the initial layer of the operating system may then verify and load succeeding layers. England says nothing about using isolated execution mode for any of those operations.

Like claim 13, claims 1, 25, and 37 also include features associated with encryption and/or decryption "while operating in isolated execution mode." England therefore does not anticipate any of the independent claims. Accordingly, since each dependent claim implicitly includes the features of its parent claim or claims, England does not anticipate any of the pending claims.

35 U.S.C. § 103(a)

The Office Action rejects claims 7-8, 19-20, 31-32, and 43-44 as being unpatentable over England. Each of those claims depends ultimately from an independent claim that involves encryption and/or decryption to be performed "while operating in isolated execution mode." England does not disclose or suggest either encrypting a value or decrypting a value "while operating in isolated execution mode." In fact, England does not disclose or suggest performing any kind of operations in isolated execution mode. England does not mention isolated execution mode at all. Consequently, England does not render any of the pending claims obvious.

For reasons including those set forth above, the Office Action fails to make out a *prima facie* case of obviousness for any of the pending claims. For these and other reasons, all pending claims are allowable.

INFORMATION DISCLOSURE STATEMENTS

The Office Action included copies of many of the information disclosure statements (IDS) that have been submitted in this application. However, two IDS

were submitted on April 5, 2002, and one of those IDSs (the one listing 21 references on two pages) was not returned in the Office Action. Also, although the Office Action included a copy of the electronic IDS (eIDS) dated August 20, 2003, that copy did not include initials from the examiner for each of the listed references. In addition, the Office Action did not include a copy of the eIDS that was submitted on December 16, 2003.

Copies of those IDSs are enclosed herewith, together with corresponding return postcards or electronic receipts. Applicants respectfully request confirmation that all references listed in those IDSs have been considered.

CONCLUSION

In view of the foregoing, claims 1-8, 10-20, 22-32, 34-44, and 46-48 are all in condition for allowance.

If the Examiner has any questions, the Examiner is invited to contact the undersigned at (512) 732-3927. Early issuance of Notice of Allowance is respectfully requested.

Respectfully submitted,

Dated: 7/14/04

Michael R. Barré
Patent Attorney
Intel Americas, Inc.
Registration No. 44,023
(512) 732-3927

c/o Blakely, Sokoloff, Taylor &
Zafman, LLP
12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1026